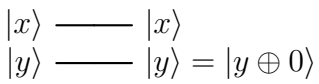
Exercise Set 3: Solution
Quantum Computation

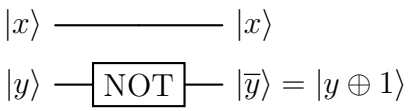
Exercise 1 *Deutsch's algorithm*

(a) The 4 oracle gates U_f are given respectively by:

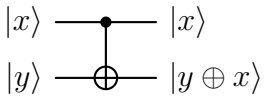
(1) For $f_1(x) = 0$:



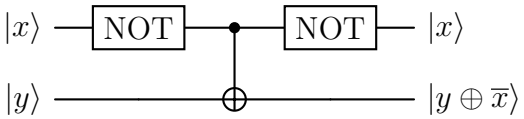
(2) For $f_2(x) = 1$:



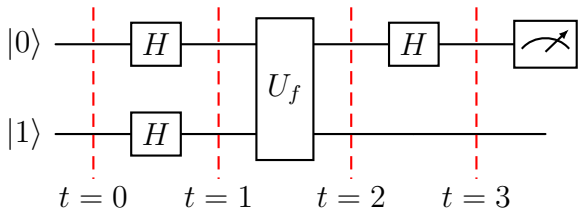
(3) For $f_3(x) = x$:



(4) For $f_4(x) = \overline{x}$:



(b) The Deutsch circuit is the following:



Let us analyze the various states:

- Initially, the state of the 2 qubits is $|\psi_0\rangle = |0\rangle \otimes |1\rangle$.
- After passage through the first Hadamard gates, the state becomes

$$|\psi_1\rangle = H|0\rangle \otimes H|1\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

- After passage through the quantum oracle U_f, the state becomes

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{2}\left(|0, f(0)\rangle - \left|0, \overline{f(0)}\right\rangle + |1, f(1)\rangle - \left|1, \overline{f(1)}\right\rangle\right)$$

- Then, after passage of the first qubit through the Hadamard gate on the right, the state becomes:

$$\begin{aligned}|\psi_3\rangle = (H\otimes I)\,|\psi_2\rangle &= \frac{1}{2^{3/2}}\Big(\,|0,f(0)\rangle + |1,f(0)\rangle - \Big|0,\overline{f(0)}\Big\rangle - \Big|1,\overline{f(0)}\Big\rangle \\ &\qquad + |0,f(1)\rangle - |1,f(1)\rangle - \Big|0,\overline{f(1)}\Big\rangle + \Big|1,\overline{f(1)}\Big\rangle\,\Big) \\ &= \frac{1}{2^{3/2}}\Big(\,|0,f(0)\rangle - \Big|0,\overline{f(0)}\Big\rangle + |0,f(1)\rangle - \Big|0,\overline{f(1)}\Big\rangle \\ &\qquad + |1,f(0)\rangle - \Big|1,\overline{f(0)}\Big\rangle - |1,f(1)\rangle + \Big|1,\overline{f(1)}\Big\rangle\,\Big)\end{aligned}$$

  after some reordering.
- Let us now analyze the state $|\psi_3\rangle$ in the two cases $f(0)=f(1)$ and $f(0)\neq f(1)$:
  - In the case where $f(0)=f(1)=x$, say, we get:

$$|\psi_3\rangle = \frac{1}{2^{3/2}}\Big(\,|0,x\rangle - |0,\overline{x}\rangle + |0,x\rangle - |0,\overline{x}\rangle\,\Big) = \frac{1}{\sqrt{2}}\left(|0,x\rangle - |0,\overline{x}\rangle\right)$$

  - In the case where $f(0)=x$ and $f(1)=\overline{x}$, say, we get:

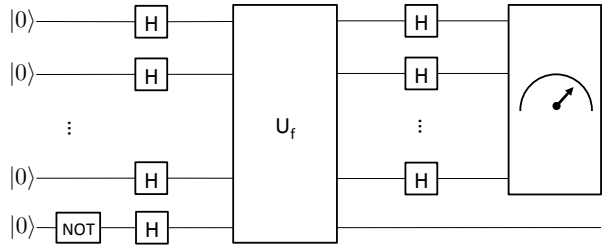
$$|\psi_3\rangle = \frac{1}{2^{3/2}}\Big(\,|1,x\rangle - |1,\overline{x}\rangle - |1,\overline{x}\rangle + |1,x\rangle\,\Big) = \frac{1}{\sqrt{2}}\left(|1,x\rangle - |1,\overline{x}\rangle\right)$$

- So finally, measuring the value of the first qubit, we obtain either $|0\rangle$ or $|1\rangle$ (each time with probability 1), which allows us to decide between the two alternatives.

(c) See the Jupyter notebook "Worksheet 3 Solutions".

Exercise 2 *Bernstein-Vazirani's algorithm*

(a) We reuse here the same circuit as in the lecture for the Deutsch-Josza algorithm:



The only thing that changes here is the prior information we have on the function f. The output state of the circuit (before the measurement) is given by

$$\begin{aligned}|\psi_4\rangle &= \frac{1}{2^n}\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}(-1)^{f(x)+x\cdot y}\,|y\rangle\otimes\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big) \\ &= \sum_{y\in\{0,1\}^n}\left(\frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot(a+y)}\right)|y\rangle\otimes\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)\end{aligned}$$

So after the measurement of the first n qubits, the outcome is state $|y\rangle$ with probability

$$\text{prob}(|y\rangle) = \left| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot(a+y)} \right|^2$$

which is equal to 1 if $y = a$ and 0 in all the other cases. Therefore the result.

(b) When adding bit b to the picture, we obtain

$$\begin{aligned}\text{prob}(|y\rangle) &= \left| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{b\oplus x\cdot(a+y)} \right|^2 \\ &= \left| \frac{1}{2^n} (-1)^b \sum_{x\in\{0,1\}^n} (-1)^{x\cdot(a+y)} \right|^2 = \left| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot(a+y)} \right|^2\end{aligned}$$

(i) The probabilities remain therefore the same as in the absence of b (which just adds a global phase), so the vector a can be equally determined.

(ii) On the contrary, b remains unknown with this scheme.

Exercise 3 *Construction of the Toffoli gate with C-NOT, H, T and S gates*

Using the first hint, we see that the circuit outputs the tensor product state $|\psi\rangle$ given by

$$|\psi\rangle = T|c_1\rangle \otimes SX^{c_1}T^\dagger X^{c_1}T^\dagger |c_2\rangle \otimes HTX^{c_1}T^\dagger X^{c_2}TX^{c_1}T^\dagger X^{c_2}H|t\rangle\,.$$

We then verify explicitly all the cases of c_1 and c_2. The calculation largely uses the fact that all the quantum gates here are unitary (*e.g.*, $TT^\dagger = T^\dagger T = I$); in particular, the gates X and H are involutory, *i.e.*, $X^2 = H^2 = I$.

For $c_1 = 0$, we have

$$\begin{aligned}|\psi\rangle &= T|0\rangle \otimes ST^\dagger T^\dagger |c_2\rangle \otimes HTT^\dagger X^{c_2}TT^\dagger X^{c_2}H|t\rangle \\ &= |0\rangle \otimes |c_2\rangle \otimes H\left(TT^\dagger\right)\left(X^{c_2}\left(TT^\dagger\right)X^{c_2}\right)H|t\rangle = |0\rangle \otimes |c_2\rangle \otimes |t\rangle\end{aligned}$$

For $c_1 = 1$ and $c_2 = 0$, let us follow the second hint:

$$XT^\dagger X = \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & 1 \end{pmatrix} = e^{-i\pi/4}T \tag{1}$$

and use this to compute

$$\begin{aligned}|\psi\rangle &= T|1\rangle \otimes SXT^\dagger XT^\dagger |0\rangle \otimes HTXT^\dagger TXT^\dagger H|t\rangle \\ &= e^{i\pi/4}|1\rangle \otimes S\left(XT^\dagger X\right)T^\dagger |0\rangle \otimes H\left(T\left(X\left(T^\dagger T\right)X\right)T^\dagger\right)H|t\rangle \\ &= e^{i\pi/4}|1\rangle \otimes e^{-i\pi/4}STT^\dagger |0\rangle \otimes |t\rangle \\ &= e^{i\pi/4}|1\rangle \otimes e^{-i\pi/4}|0\rangle \otimes |t\rangle = |1\rangle \otimes |0\rangle \otimes |t\rangle\end{aligned}$$

Finally, for $c_1 = c_2 = 1$, we compute, using repeatedly (1):

$$\begin{aligned}|\psi\rangle &= T|1\rangle \otimes SXT^\dagger XT^\dagger |1\rangle \otimes HTXT^\dagger XTXT^\dagger XH|t\rangle \\ &= e^{i\pi/4}|1\rangle \otimes e^{-i\pi/4} STT^\dagger |1\rangle \otimes e^{-i\pi/2} HT^4 H|t\rangle \\ &= e^{i\pi/4}|1\rangle \otimes e^{i\pi/4}|1\rangle \otimes e^{-i\pi/2} X|t\rangle\end{aligned}$$

as

$$T^4 = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi}\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$

and therefore

$$HT^4H = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}0 & 2\\ 2 & 0\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = X$$

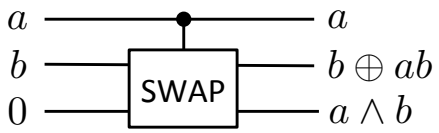
Finally, this gives

$$|\psi\rangle = |1\rangle \otimes |1\rangle \otimes |\bar{t}\rangle$$

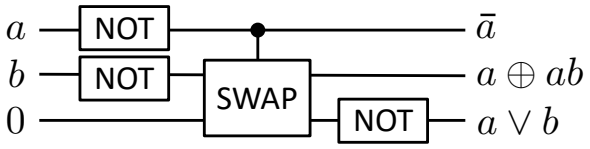
as expected.

Exercise 4 *Fredkin gate*

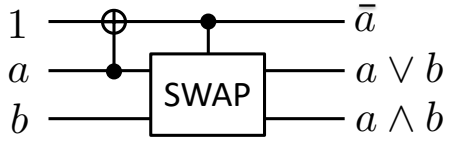
(a) The AND gate can be represented as follows with only the Fredkin gate:



The OR gate is then given by (using $a \vee b = \mathrm{NOT}\big(\mathrm{NOT}(a) \wedge \mathrm{NOT}(b)\big)$):



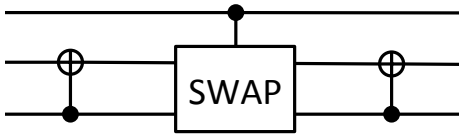
Another solution for both AND and OR uses a combination of CSWAP and CNOT:



(b) The Fredkin is a controlled SWAP which swap's the last two bits if the first one is equal to 1. Thus we find

$$\mathrm{CSWAP} = \begin{pmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\end{pmatrix}.$$

(c) From the matrix representation of Fredkin, we see that to obtain the matrix representation of CCNOT, we have to permute on rows 5,6,7,8. With a bit of thought (see below for some extra help) one can find that the CCNOT gate can be represented as



Another way is by noting that

$$\begin{aligned}
&\text{CNOT}|x, y\rangle = |x, x \oplus y\rangle, \\
&\text{CCNOT}|x, y, z\rangle = |x, y, z \oplus xy\rangle, \\
&\text{CSWAP}|x, y, z\rangle = |x, y \oplus x(y \oplus z), z \oplus x(y \oplus z)\rangle.
\end{aligned}$$

Thus an input $|x, y, z\rangle$ becomes $|x, y\oplus z, z\rangle$ after the first CNOT gate, $|x, y\oplus z\oplus xy, z\oplus xy\rangle$ after the Fredkin gate and $|x, y, z \oplus xy\rangle$ after the second CNOT gate.

Extra help. While it is easy to verify that a given circuit implements a desired operation, constructing such a circuit can be less obvious. Let us therefore derive the intermediate steps explicitly. In this example, the matrix representation is particularly useful because all the gates involved are permutation matrices. We denote by r_i the i-th row of the matrix, with $i = 0, \ldots, 7$.

The Toffoli and Fredkin gates are

$$\text{CCNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \qquad \text{CSWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and correspond to the permutations

$$\text{CCNOT} : r_6 \leftrightarrow r_7, \qquad \text{CSWAP} : r_5 \leftrightarrow r_6.$$

The two-qubit CNOT gates are

$$\text{CNOT}_{0\to1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \text{CNOT}_{1\to0} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

and correspond to the permutations

$$\text{CNOT}_{0\to1} : r_2 \leftrightarrow r_3, \qquad \text{CNOT}_{1\to0} : r_1 \leftrightarrow r_3.$$

Embedding them into three qubits gives

$$I \otimes \mathrm{CNOT}_{0\to 1} : r_2 \leftrightarrow r_3,\ r_6 \leftrightarrow r_7,$$

and

$$I \otimes \mathrm{CNOT}_{1\to 0} : r_1 \leftrightarrow r_3,\ r_5 \leftrightarrow r_7.$$

We use the latter to move the rows we want to swap, $r_5 \leftrightarrow r_7$, then apply CSWAP ($r_5 \leftrightarrow r_6$), and finally undo the first permutation. All intermediate swaps cancel except $r_6 \leftrightarrow r_7$, which is precisely the action of the Toffoli gate. Hence

$$\boxed{\mathrm{CCNOT} = (I \otimes \mathrm{CNOT}_{1\to 0})\ \mathrm{CSWAP}\ (I \otimes \mathrm{CNOT}_{1\to 0})}.$$